(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/088893 A1

(51) International Patent Classification^7: H04L 9/00

(21) International Application Number: PCT/US2004/004117

(22) International Filing Date: 13 February 2004 (13.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (*for all designated States except US*): PSY-CRYPT, INC. [US/US]; Suite 213, 2635 North First Street, San Jose, CA 95139 (US).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): WATANABE, Masashi [JP/JP]; 49-1, Machisuji, Iwawaki, Hanoura-cho, Naka-gun, Tokushima (JP).

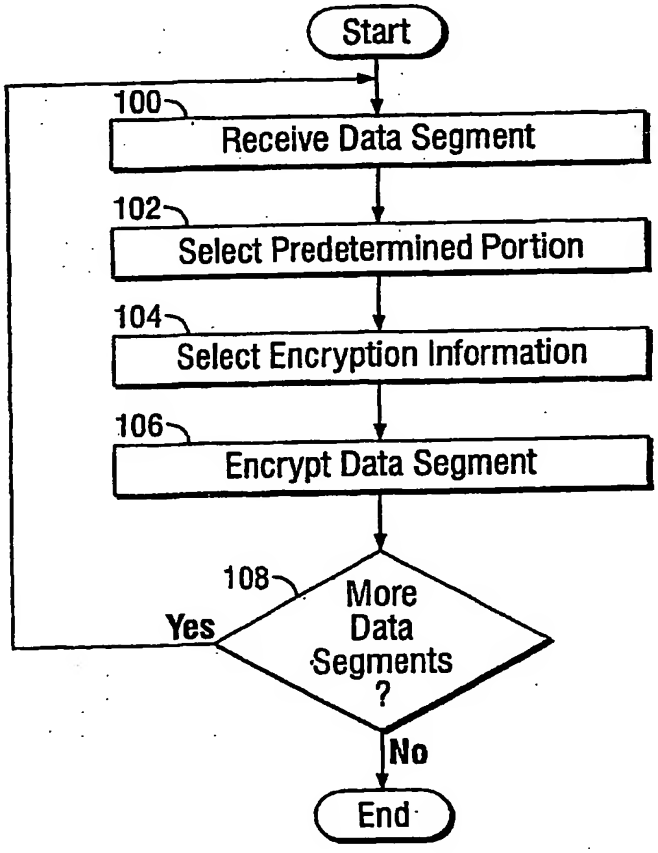
(74) Agents: RITCHIE, David, B. et al.; Thelen Reid & Priest, LLP, P.O. Box 640640, San Jose, CA 95164-0640 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR CRYPTOGRAPHICALLY PROCESSING DATA



(57) Abstract: A method and apparatus cryptographically process data including a plurality of data segments. The cryptographic process includes (a) receiving a plurality of data segments (100), (b) selecting, for each data segment, a set of encryption information based on data contained in a predetermined portion of the data segment to be encrypted (102, 104), and (c) encrypting each data segment using the set of encryption information selected for the data segment (106). At least one of an encryption algorithm, an encryption key, and an encryption parameter may be changed for each data segment based on the data contained in the predetermined portion. The predetermined portion may include a first predetermined portion for selecting a first set of encryption information, and a second predetermined portion for selecting a second set of encryption information, the encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.